FORSCHUNGSZENTRUM JÜLICH GmbH
Zentralinstitut für Angewandte Mathematik
D-52425 Jülich, Tel. (02461) 61-6402

Interner Bericht

Aufbau von NT-basierten Arbeitsgruppen in TCP/IP-Netzen am Beispiel Forschungszentrum Jülich

Werner Anrath, Rainer Grallert

FZJ-ZAM-IB-9802

März 1998
(Stand 10.03.1998)

Inhaltsverzeichnis

Abbildungen

Tabellen

1 Einführung

Im vorliegenden Bericht werden Aspekte und Erfahrungen zur Integration von Windows NT in TCP/IP-Netze am Beispiel des lokalen Netzwerks im Forschungszentrum Jülich beschrieben. Weiterhin werden neben der Analyse der Netzwerkaspekte mögliche Organisationsformen von Windows NT-Systemen in Arbeitsgruppen und Domänen in diesem Kontext untersucht. Diese Untersuchung liefert Kriterien für zukünftige Entscheidungen, welche Rolle bzw. Aufgaben das ZAM, externe Service-Anbieter und letztendlich die Organisationseinheiten selbst in einem einheitlichen organisierten Betriebskonzept für standardisierte NT-Arbeitsgruppen wahrnehmen können.

2 Grundlagen zu Windows NT Netzwerken

2.1 Einführung in die Netzwerkgrundbegriffe

In diesem Kapitel werden Grundbegriffe zum Netzwerkbetriebssystem Windows NT erklärt. An dieser Stelle sollen neben Grundbegriffen und der entsprechenden Hintergrundinformation spezifische Aspekte zur Netzanbindung von NT-Systemen im Forschungszentrum Jülich unmittelbar dargelegt werden.

2.2 Windows NT Server und Windows NT Workstation

Das Betriebssystem Windows NT wird in zwei Varianten ausgeliefert. Die Variante **NT - Workstation** ist für die Nutzung von **Desktop-Applikationen** optimiert; die Bedienoberfläche ist für den Benutzer mit der Windows 95 Oberfläche gleich. Die Implementierung **NT-Server** ist für **Datei- und Druckdienste** optimiert. Neben diesen klassischen Diensten sind für NT-Server weitere Dienste implementiert und installierbar, so z.B. ein Web-Server.

Für jeden Client, der auf Datei- und Druckdienste eines NT-Servers zugreift, muß aus rechtlichen Gründen eine sogenannte *Client Access License* vorhanden sein.

Dem Betriebssystem Windows NT-Server kann bei der Installation entweder die Rolle *Server* oder *Domain-Controller* zugeteilt werden. Gegenüber einem NT-System in der Rolle *Server* übernimmt ein sogenannter *Domain-Controller* zusätzlich die Steuerung aller Sicherheitsfunktionen zur Zugriffskontrolle in einem Verbund aus NT-Systemen. Dies vereinfacht die Benutzerverwaltung, da diese zentral auf dem *Domain-Controller* erfolgt.

Merkmal	NT-Workstation	NT-Server
Einsatz	Client OS, Desktop	Server OS
Benutzeroberfläche	Windows 95	Windows 95
Fehlertoleranz	nein	Software-RAID
SMP-Unterstützung	2	4
Client-Verbindungen	10	unbegrenzt
WINS / DHCP / DNS	- / - / -	+ / + / +
Internet Information Server	nein	ja
Verwaltungsassistent	nein	ja
Backoffice lauffähig	nein	ja

Tabelle 1 – Vergleich Workstation/Server

2.3 Arbeitsgruppen und Domänen

2.3.1 Arbeitsgruppen

Eine Arbeitsgruppe besteht aus einem oder mehreren Windows-Systemen, die sich unter einem gemeinsamen Arbeitsgruppen-Namen im Netzwerk identifizieren und somit in einer sogenannten *Browse-Liste* in der Netzwerkumgebung eines Rechners erscheinen. Zum Anzeigen kann das Icon Netzwerkumgebung oder der Windows-Explorer geöffnet werden.

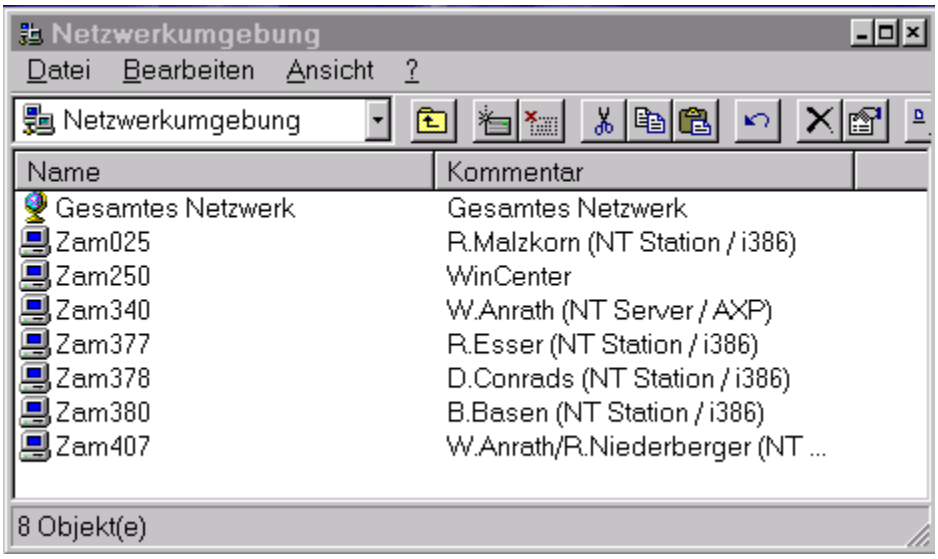

Abbildung 1 – Netzwerkumgebung im Windows Explorer/Desktop-Icon

Eine solche Arbeitsgruppe kann Windows 95, Windows NT Workstation, Windows NT Server wie auch UNIX-Rechner mit einer entsprechenden NetBIOS over TCP/IP Implementierung enthalten. Der Zugriff auf Resourcen basiert auf der sogenannten Share-Level-Security. Beispiel: Gibt ein Windows 95 Anwender einen lokal angeschlossenen Drucker frei, so kann er die Benutzung durch ein Kennwort reglementieren, das lokal gespeichert wird; für den Druckerzugriff von anderen Windows-Systemen ist dieses Kennwort erforderlich. Soll beispielsweise später der Druckzugriff auf einen anderen Benutzerkreis beschränkt werden, ist ein neues Kennwort erforderlich. Insofern NT-Systeme und UNIX-Systeme in einer Arbeitsgruppe sind, müssen Benutzer-Accounts gegebenenfalls auf jedem dieser Systeme mehrfach administriert werden, falls der Zugriff auf diese *Multiuser-Systeme* unter vorgegebenen Identitäten (Benutzername + Kennwort) erfolgt.

2.3.2 Domänen

Eine weiterentwickelte Form der Zugriffssteuerung und der Benutzerverwaltung bietet in Verbindung mit Windows NT Server das sogenannte NT-Domänenmodell. Eine NT-Domäne ähnelt einer Arbeitsgruppe, jedoch ist eine zentrale Sicherheitssteuerung und Benutzerverwaltung auf einem speziell installierten Windows NT Server implementiert. Der Zugriff auf freigegebene Ordner und Drucker basiert auf zentral administrierten Access-Control-Lists, kurz ACLs. Damit wird eine flexible Steuerung der Zugriffe ermöglicht; das Ändern und Mitteilen von Kennworten ist überflüssig. Benutzeraccounts müssen nur einmal auf dem Primary Domain Controller eingerichtet werden.

Alle NT-Workstations oder NT-Server haben in der Domäne ein sogenanntes Computer-Konto, das den jeweiligen Rechner gegenüber dem Primary Domain Controller eindeutig als Mitglied der NT-Domäne identifiziert; Vortäuschen einer Identität durch IP-Adresse und Name sind damit unterbunden.

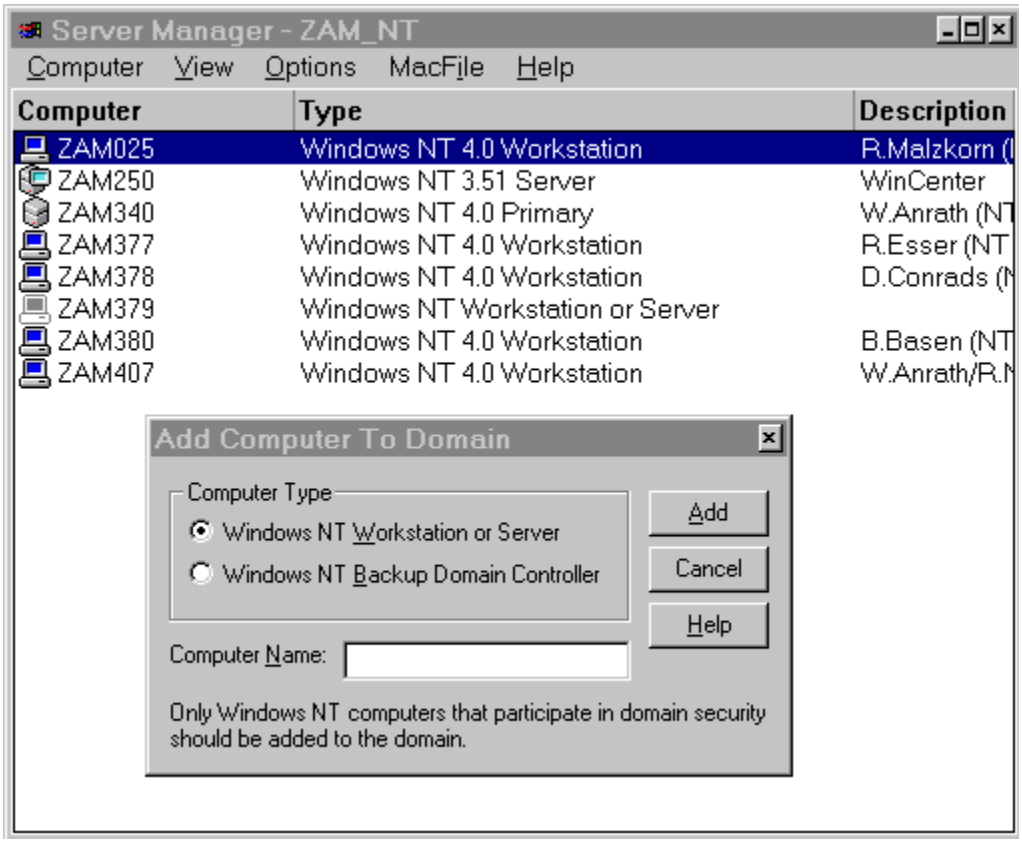

Abbildung 2 – Computer-Konten in einer NT-Domäne

Werden statt Windows NT Workstation oder Windows NT Server andere Betriebssysteme in der Domäne verwendet, kann zwar ein Datenaustausch mit der Domäne erfolgen, jedoch verfügen diese Systeme nicht über die Anmeldesicherheit von Windows NT.

Insbesondere gilt für Windows 95, daß bei der Übereinstimmung des Arbeitsgruppennamens mit einem Domänennamen der entsprechende **Windows 95** Rechner in der Browse-Liste der Domäne aufgeführt wird, aber der Zugriff auf seine eigenen lokalen Ressourcen (Dateien u. Drucker**) unterliegt nicht der zentralen Sicherheitssteuerung**.

Zwischen Domänen können sogenannte Vertrauensstellungen definiert werden. Dadurch können Benutzer einer Domäne auch Zugriffsrechte auf Ressourcen einer anderen Domäne erhalten (ohne explizit als weiterer Benutzeraccount eingerichtet zu sein).

2.3.3 Vertrauensstellungen

Soll einer Anwender auf Resourcen in zwei verschiedenen Domänen (zwei Einzeldomänen) zugreifen, so muß dieser Anwender in jeder der beiden Domänen einen gültigen Benutzer-account (Konto) haben.

Eine Alternative dazu besteht in der Definition einer sogenannten Vertrauensstellung. Dabei vertraut im einfachsten Fall eine Domäne B einer Domäne A. Diese Vertrauensstellung ist einseitig. Falls nun ein Benutzeraccount der Domäne A in eine sogenannte *Globale Gruppe* (Konzept der NT-Benutzerverwaltung) der eigenen NT-Domäne aufgenommen wird, kann der Benutzer in der anderen Domäne erkannt werden und dort Rechte haben. Eine *Globale*

Gruppe umfaßt eine Anzahl von Benutzerkonten einer Domäne; diesen Benutzern können damit Zugriffsrechte und Berechtigungen für die Nutzung von Ressourcen in anderen Domänen erteilt werden. Ein sogenannte *Lokale Gruppe* kann Benutzerkonten und globale Gruppen aus einer oder mehreren Domänen enthalten. Zugriffsrechte und Berechtigungen sollten nur an lokale Gruppen vergeben werden.

2.4 Windows NT Protokolle und Netzdienste

2.4.1 Grundregeln im Forschungszentrum Jülich

Als Kommunikationsprotokoll wird im lokalen Netzwerk des Forschungszentrums TCP/IP eingesetzt. Die Verantwortung für den Betrieb der erforderlichen Infrastruktur für IP (Internet Protocol) liegt beim ZAM. Die Verwendung von TCP/IP garantiert Windows NT Systemen das problemlose Zusammenspiel mit anderen Systemen im Forschungszentrum und die Nutzung zentraler Dienste wie z.B. Datensicherung und Druckausgabe. Andere Protokolle wie z.B. NetBEUI oder IPX/SPX dürfen im Backbone-Netz nicht verwendet werden; dabei sollte schon aus eigenem Interesse lediglich das mittlerweile in NT als Standardprotokoll vorgesehene TCP/IP installiert sein, um Nebeneffekte und Fehlerquellen durch falsche Protokollbindungen vorweg auszuschließen.

2.4.2 NetBIOS over TCP/IP

Das API (Application Program Interface) für die in der Microsoft-Welt vorgesehenen Möglichkeiten des Datei- und Drucker-Sharing ist NetBIOS**. NetBIOS** ist, entgegen dem früher verbreiteten Sprachgebrauch, kein Kommunikationsprotokoll sondern lediglich eine **Schnittstelle** für Netzwerkanwendungen. Diese Schnittstelle benötigt eine Bindung an ein sogenanntes Transportprotokoll; dieses **Transportprotokoll** muß im Forschungszentrum Jülich **TCP/IP** sein.

Andere Transportprotokolle wie das ältere NetBEUI (NetBIOS Extended User Interface) dürfen nicht installiert werden.

2.4.3 Winsock-Anwendungen

Anwendungen wie Telnet (Virtual Terminal) oder FTP (File Transfer) nutzen zur TCP/IP-basierten Kommunikation die sogenannte WINSOCK-Schnittstelle. Diese zweite Schnittstelle wird i.a. von solchen Applikationen genutzt, die aus der UNIX-Welt stammen.

2.5 Weitere Begriffe

2.5.1 WINS Server und DNS Server

Für die Nutzung von Netzdiensten nehmen die Namensdienste WINS (Windows Internet Name Service) und DNS (Domain Name System) eine Schlüsselstellung ein. Nach der Konfiguration dieser Komponenten kann der Anwender mit symbolischen Host-Namen am Internet angeschlossene Systeme adressieren. Dabei optimiert die WINS-Komponente die Namensauflösung bei der Nutzung von NetBIOS-Anwendungen in Bezug auf Antwortzeit und Schonung der Netzressourcen; Winsock-basierte Anwendungen (ftp, telnet) nutzen dagegen eine von UNIX-Systemen abgeleitete Strategie und verwenden das sogenannte DNS. Fällt eine Server-Komponente aus, wird wechselseitig versucht, die Zuordnung *Computer-Name – IP-Adresse* über den jeweils anderen Namensdienst zu erhalten.

Um Mißverständnissen vorzubeugen, sei an dieser Stelle ausdrücklich darauf hingewiesen, daß hier der Ausdruck *Domain* in keinem Zusammenhang mit dem Begriff Windows NT Domäne steht.

DNS- und WINS-Server werden vom ZAM betrieben; bei der Netzwerkkonfiguration muß der NT-Administrator lediglich bei der Client-Konfiguration die IP-Adressen der Server angeben. Der noch aus älteren LAN-Manager Implementierungen bekannte *lmhosts*-File sollte nicht eingesetzt werden.

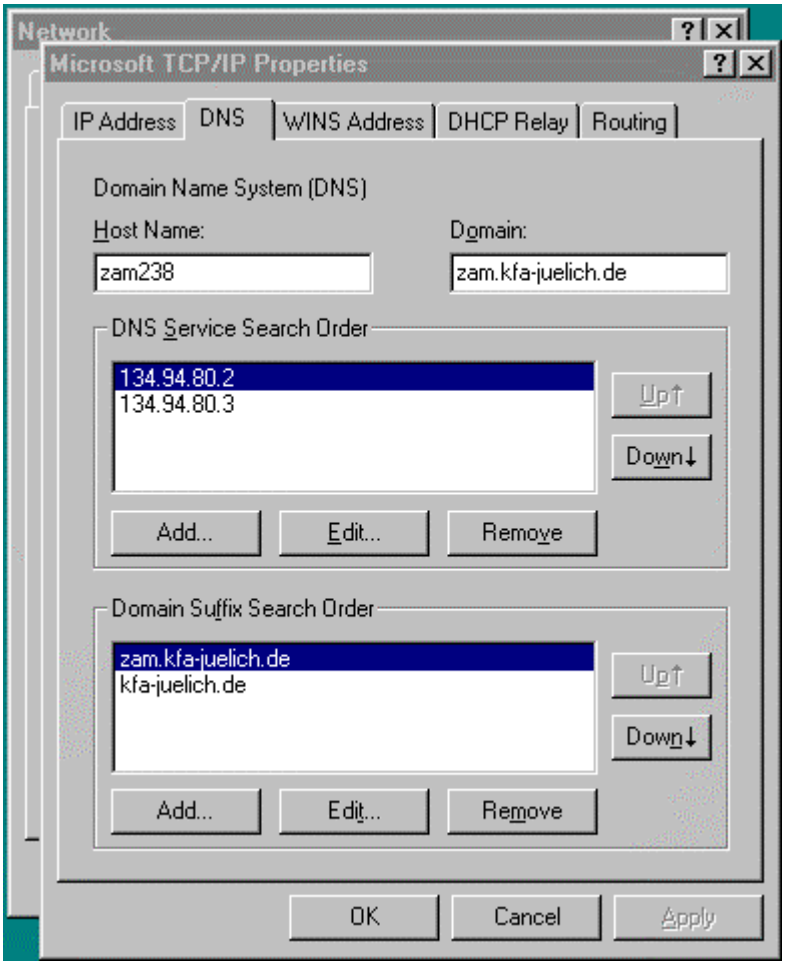

Abbildung 3 – DNS Client Konfiguration

2.5.2 Master Browser

Der sogenannte Master-Browser stellt **automatisch** eine Liste aller Rechner zusammen, die unter einem Arbeitsgruppennamen bzw. einem Domänennamen organisiert sind; eine explizite Konfiguration durch einen Administrator ist nicht erforderlich! Beim Zugriff auf die Netzwerkumgebung in einem Betriebssystem wie Windows 95 oder Windows NT liefert der Master-Browser die Liste der aktiven Rechner in der Arbeitsgruppe. Welcher Rechner die Rolle des Master-Browsers in einer Arbeitsgruppe übernimmt, hängt von der Priorisierung der Betriebssysteme ab. Ein Rechner unter Windows NT Server hat bei der Auswahl des Master-Browser die höchste Priorität. Die Master Browser bauen die Browse-Liste anhand von regelmäßigen BROADCAST-Meldungen der Rechner einer Arbeitsgruppe auf.

Eine manuelle Anpassung dieser Mechanismen über Registry-Modifikationen ist nicht zu empfehlen. Die Browser-Funktionen innerhalb einer Arbeitsgruppen arbeiten nur einwandfrei,

wenn alle Systeme der Arbeitsgruppe das gleiche Transportprotokoll, in unserem Fall also TCP/IP, benutzen.

Die folgende Abbildung zeigt den Master-Browser der Arbeitsgruppe *ZAM_HQ*, der Arbeitsgruppe *ZAM_KS* sowie der NT-Domäne *ZAM_NT*. Der Master-Browser der Arbeitsgruppe ZAM_HQ ist momentan ein Windows 95 Rechner, in der Arbeitsgruppe ZAM_KS hat ein UNIX-System mit der NetBIOS over TCP/IP-Implementierung Samba diese Rolle übernommen. In der Domäne ZAM_NT hat der Primary Domain Controller den Auswahl-Prozeß gewonnen.

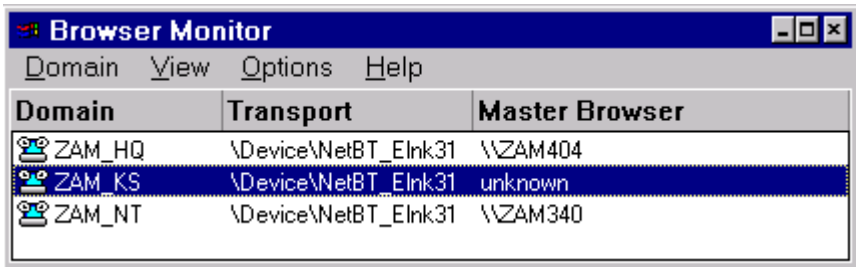

Abbildung 4 – Browser Liste

2.5.3 Domain Master Browser

Die Rolle des Domain-Master-Browsers ist spezifisch für eine WINDOWS NT-Domäne. Falls die in der Domäne organisierten Rechner über verschiedene TCP/IP-Subnetze verteilt sind, synchronisiert der Domain Master Browser **automatisch** die entsprechenden Listen der Master Browser in den jeweiligen TCP/IP-Subnetzen, so daß alle Rechner der Domäne in der Netzwerkumgebung sichtbar sind. Die aktuellen Implementierung in Windows NT 4.0 und Windows 95 bedingen bei diesem Vorgang teilweise Wartezeiten bis zu 51 Minuten.

Als vorteilhaft erweist sich auf jeden Fall die Zusammenlegung der Domänen-Mitglieder (NT-Systeme) in ein TCP/IP-Subnetz.

2.6 DHCP Server

In Firmen und Organisationen, in denen Mitarbeiter mit mobilen Windows-Systemen an verschiedenen Standorten arbeiten, kann mit Hilfe von DHCP, Dynamic Host Configuration Protocol, beim Starten der mobilen Arbeitsplätze in den Standorten, und damit auch in einem jeweils anderen TCP/IP-Kontext, die TCP/IP-Konfiguration dynamisch durch einen DHCP-Server erfolgen.

Diese Art der TCP/IP-Konfiguration soll im Forschungszentrum Jülich nicht angewendet werden, weil dadurch die Unterstützung der Netz-Anwender bei der Netzwerkdiagnose und Fehlerbehebung unmöglich wird.

2.7 Network Client Administration

Diese Komponente ist Bestandteil der NT-Server Implementierung und bietet die Installation von Windows Betriebssystemen über das Netzwerk an; diese Installation kann auch TCP/IP basierend erfolgen und ist nicht an Subnetzgrenzen gebunden. Die generierten Startdisketten basieren auf DOS-TSR-Programmen. Ferner müssen Treiber für neuere Netzwerk-Adapter manuell eingearbeitet werden. Je nach Client-Hardware ist auf die Konflikt-Freiheit beim Zuweisen von Interrupts und I/O-Adressen zu achten. Der Einsatz dieser Komponente empfiehlt sich somit nur bei der Installation vieler gleichartiger Clients mit möglichst identischer Hardware.

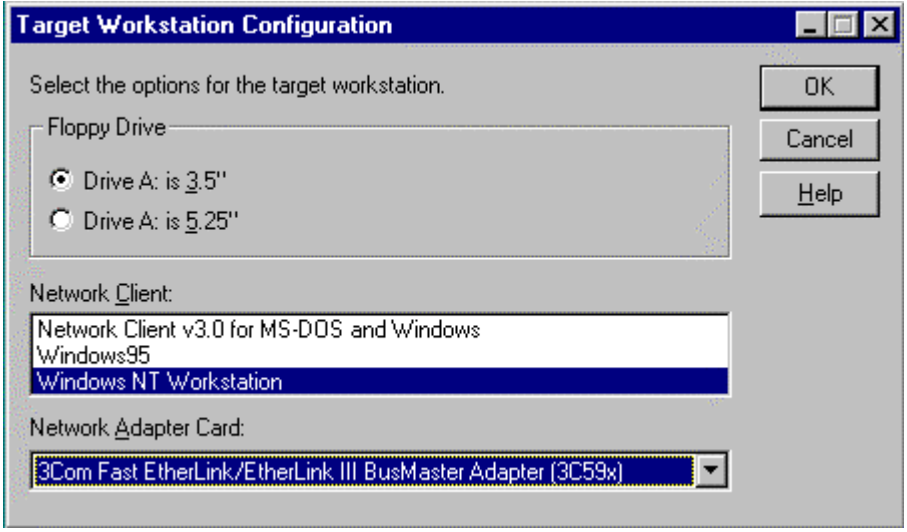

Abbildung 5 – Network Client Administration

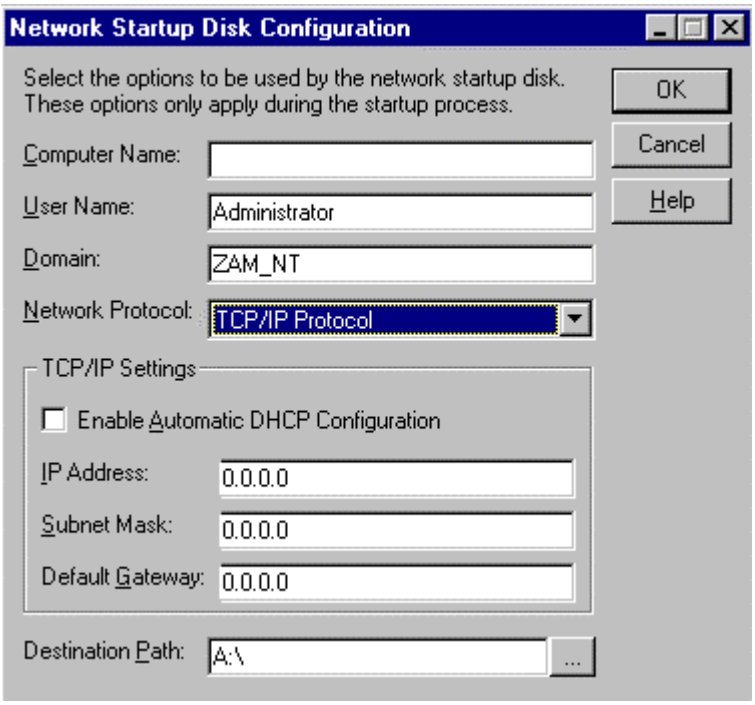

Abbildung 6 – Network Startup Disk

3 Ausgangssituation im ZAM

3.1 Der zentrale Server PCSRV

3.1.1 PC-Software Distribution und Laufzeitsysteme

Ende 1997 wurde durch die Inbetriebnahme eines AlphaServer 1000A und dem Betriebssystem Digital UNIX als PC-Server eine deutliche Leistungssteigerung beim Zugriff auf zentral angebotene Software und Dokumentvorlagen für Windows erzielt. Die Interoperabilität mit den Windows-Systemen wird durch die Public Domain Software Samba erreicht; dieses Produkt ist eine Implementierung von NetBIOS over TCP/IP für UNIX-Rechner. Eine RAID-basierte Massenspeicherkonfiguration reduziert die Fehleranfälligkeit. Hohe CPU-Leistung und eine angepaßte Hauptspeicherkapazität garantieren attraktive Antwortzeiten. Im Forschungszentrum ist dieser Service weitläufig als das Netzwerklaufwerk Q-Disk bekannt. Viele der für Windows 95 angebotenen Software-Produkte funktionieren ebenfalls auf NT-Systemen.

Neben dem Zugriff auf Basis von NetBIOS und dem Transportprotokoll TCP/IP kann an dieser Stelle nicht auf NFS verzichtet werden, da noch einige hundert ältere Windows-Systeme und auch UNIX-Systeme mit PC-Emulationen zugreifen. Dieser Umstand bedingte 1997 die Entscheidung zugunsten eines UNIX-basierten Systems, da insbesondere die Erfahrungen mit diversen NFS-Produkten für NT-Server unbefriedigend ausfielen.

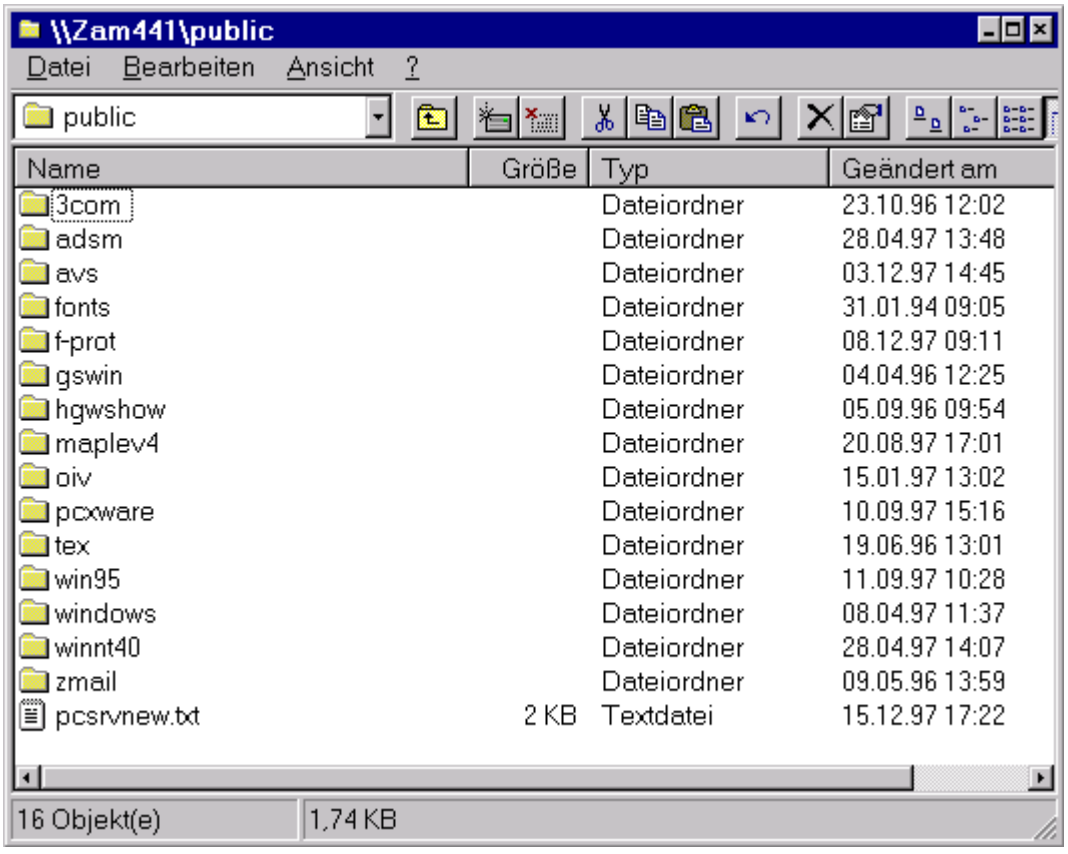

Abbildung 7 – PCSRV und Q-Disk

3.2 WINS

Die bisher installierten Samba-Versionen bieten neben der Unterstützung der oben genannten Dienste den Betrieb als Windows Internet Name Service an. Die Nutzung dieses zentralen Namensdienstes ist für Windows 95 in einer entsprechenden TKI dokumentiert. Im Kontext von Windows 95 und NT 4.0 Implementierungen ist diese WINS-Funktionalität völlig ausreichend in Bezug auf Effizienz und Funktionalität. Die Implementierung neuer Funktionen und deren Brauchbarkeit in zukünftigen Samba-Versionen muß gesondert betrachtet werden; je nach Situation muß gegebenenfalls der jetzige zentrale UNIX-basierte Server durch ein NT-System ergänzt werden, um einen effizienten NetBIOS over TCP/IP Betrieb auch weiterhin zu gewährleisten.

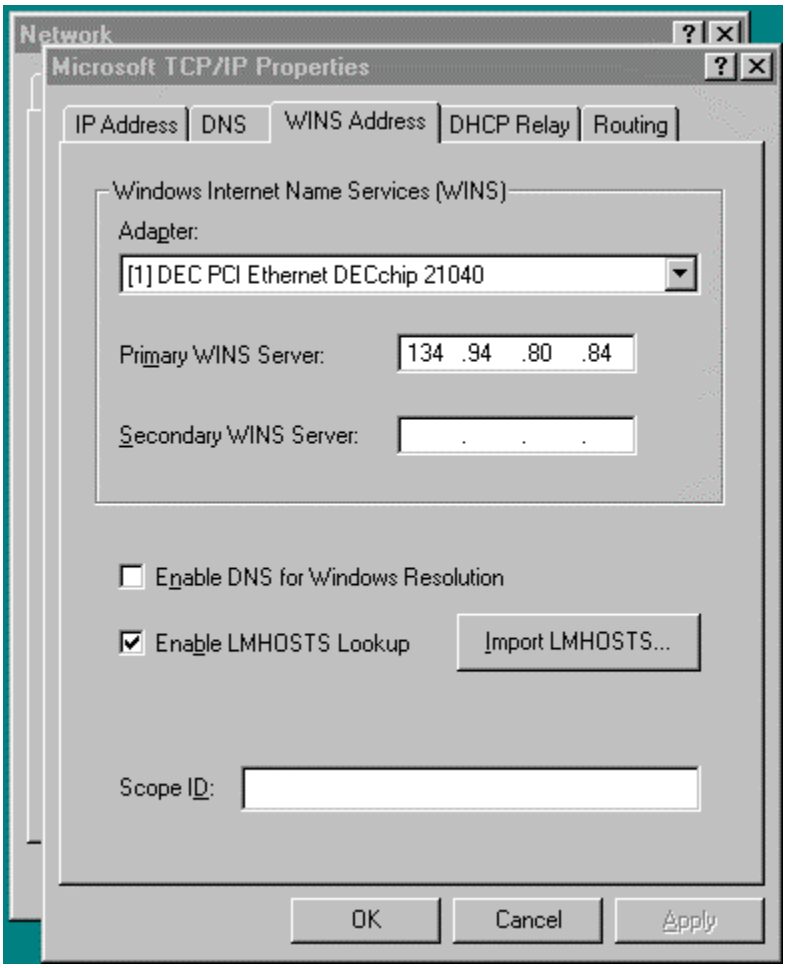

Abbildung 8 – WINS Client Konfiguration

4 Testumgebung im ZAM

4.1 NT-Workstations oder NT-Server in einer Arbeitsgruppe

Erste Erfahrungen und Kenntnisse bezüglich der Installation und Konfiguration von Windows NT-Workstations und NT-Server-Systemen wurden anhand dieses einfachen Modells, das sich **automatisch** aus der Netzwerkanbindung eines Windows-Systems ergibt, erarbeitet. Durch Wahl eines entsprechenden Arbeitsgruppennamens erfolgt die Zuordnung zu einer Arbeitsgruppe. Hier wurden im weiteren Sinne noch keine Funktionen wie Domain-

Controller, Network Client Administration, Internet Information Services (IIS) und zentrale Sicherheitssteuerung benutzt, die ausschließlich von einem NT-Server oder insbesondere einem Domain-Controller bereitgestellt werden können. Folgende Punkte sind besonders herauszustellen:

- als Netzwerkprotokoll wurde ausschließlich **TCP/IP** benutzt.
- die Funktionstüchtigkeit aller standardmäßig vorhandenen Netzdienste wurde in Verbindung mit TCP/IP getestet, insbesondere auch solche, die das NetBIOS-API verwenden.
- die mit NT 4.0 ausgelieferte TCP/IP-Implementierung konnte problemlos im JuNet eingesetzt werden.
- die Konfiguration weiterer Transportprotokolle führte nachweislich zu Störungen, insbesondere beim Browsing.
- als Dateisystem wurde **NTFS** (NT File System) genutzt (statt FAT).
- die **Verwaltung der Benutzeraccounts** erfolgte **dezentral auf** dem **jeweiligen System**, in Bezug darauf sprechen wir im folgendem von einem Standalone System
- jeder **Benutzeraccount** erhielt ein eigenes **Home-Directory** zur Speicherung von Dateien, die Mailbox wird ebenfalls in diesem Directory abgelegt; der gesamte Bereich wird über **ACL** (Access Control List) vor unberechtigten Zugriffen geschützt.
- Anwendungssoftware, z.B. MS-Office wurde lokal installiert.
- **der Zugriff auf zentrale Dienste funktioniert** (u.a. Datensicherung, Drucken, Q-Disk).

Gegenüber Windows 95 steht dem Anwender damit ein System zur Verfügung, das aufgrund der besseren Dateisystemtechnologie (NTFS) eine bessere Datenintegrität bietet. Ferner muß der Anwender einen richtigen Login-Vorgang mit einer gültigen Kombination Benutzername-Kennwort durchlaufen. Daß NT 4.0 das besserere Multi-Tasking Betriebsystem ist, sticht bei den üblichen Office-Anwendungen nicht unmittelbar hervor; jedoch ist diese Eigenschaft für den Betrieb als Datei-, Druck- und Applikationsserver offensichtlicher und unbedingt notwendig. Positiv fiel während dieser Testphase zudem die gut funktionierende Hardwareüberwachung und Fehlererkennung auf.

Mehrere, auf diese Art installierte Workstations, bilden in der gleichen Weise eine **Arbeitsgruppe** wie bei einer Windows 95 Installation, dieser Zusammenhang ergibt sich **automatisch** bei der Wahl eines gleichen Arbeitsgruppennamens.

4.2 Testaufbau der Domänen im ZAM

Im weiteren Verlauf des Projektes wurden die NT-Systeme in zwei einfache **unabhängige Einzeldomänen** überführt. Damit sollte geprüft werden, ob die Installations- und Konfigurationsarbeiten auf den einzelnen Desktop-Systemen (NT-Workstations) vereinfacht und alltägliche Administrationsaufgaben wie Benutzerverwaltung und Datensicherung optimiert werden können. Die zweite Domain wurde zeitweise zum Testen von Vertrauensstellungen benutzt. Die **NT-Server** mußten für die Rolle des **Primary Domain Controller neu installiert** werden. Die Domain Controller übten ferner die Rolle eines zentralen File-Servers für die Domänen-Mitglieder aus. Zur Verschärfung der Testbedingungen wurden die beteiligten Systeme ferner über TCP/IP-Subnetzgrenzen hinweg verteilt Diese Maßnahme sollte eventuelle Schwachstellen in internen Kommunikationsanwendungen zur Umsetzung der Domänenstruktur aufdecken. Die Konfiguration, die sich in Folge als praxisgerecht erwies, wird in den nachfolgenden Kapiteln vorgestellt.

4.3 Netzwerkkonfiguration

Die Netzwerkkonfiguration nutzte ausschließlich **TCP/IP als Transportprotokoll**. Die aus Computer-Name und Domain-Name bestehende **NetBIOS-Identifikation** wurde an den **Internet-Host-Namen** angepaßt. Der **Domain-Name** wurde aus dem Namen der Organisationseinheit abgeleitet. Da im ZAM für Arbeitsgruppen als Konvention ZAM_*Abteilungskürzel* vereinbart ist, ergeben sich beispielsweise Arbeitsgruppennamen wie ZAM_KS (d.h. ZAM, Abteilung Kommunikationssysteme) oder ZAM_HQ. Als Domain-Namen für die Untersuchungen in diesem Projekt wurden die Kunstworte ZAM_MS und ZAM_NT gewählt. Im Hinblick auf die Internet-Standards und dem ergänzenden Zusammenspiel von WINS und DNS sollte künftig konform zu RFC 819 ***Organisationseinheit-Abteilung*** (z.B. ZAM-KS) verwendet werden. Diese schlichte Formalisierung erlaubt die Registrierung der Domain im statischen Namensraum des DNS im Forschungszentrum Jülich, wobei diesem Namen dann der Internet-Host-Name des Primary Domain Controller zugeordnet wird. Vorteile sind daraus:

- die Funktion eines Internet-Rechners als Domain-Controller ist in den Netzwerk-datenbanken erfaßt (und damit der Domain-Name).
- der Login-Vorgang über Subnetzgrenzen hinweg ist ohne lmhosts-Datei möglich.
- höhere Robustheit beim Browsing (bei WINS Ausfall).

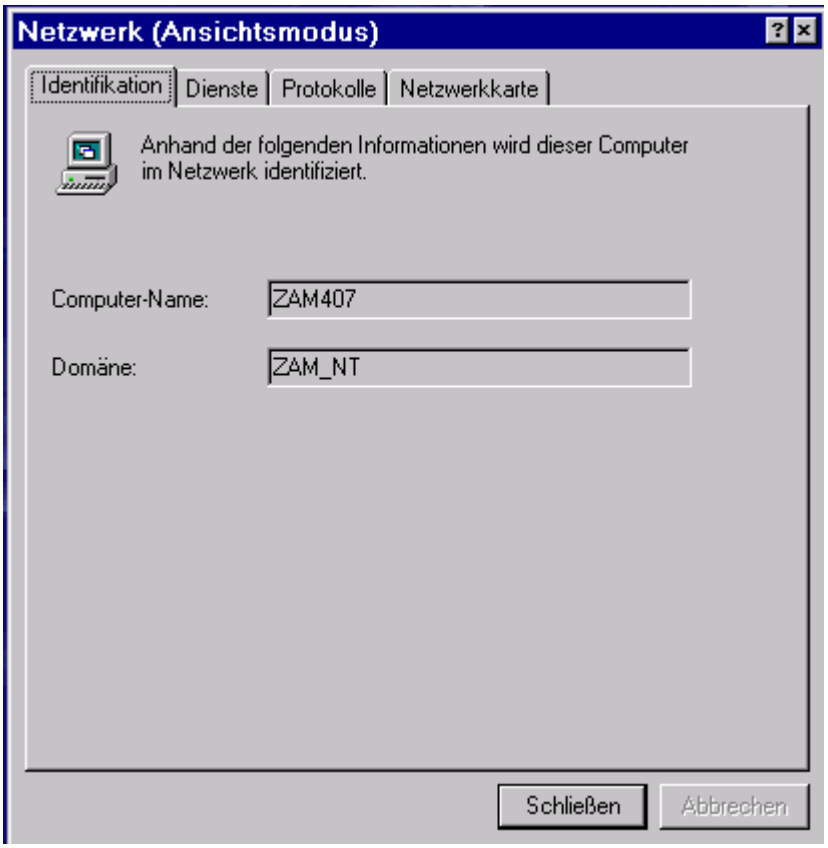

Abbildung 9 – Netzwerk-Identifikation

Bemerkung: die Vergabe der Arbeitsgruppennamen ist derzeit nicht zentral geregelt, empfohlen werden bisher Namen wie ZAM_KS; der zusätzliche Eintrag nach der oben vorgeschlagenen Art (RFC konform) kann bei der Beantragung einer Internet-Adresse im ZAM direkt mit erledigt werden.

4.4 Benutzerverwaltung

Die Benutzerverwaltung sowie die Steuerung der Zugriffsrechte erfolgte zentral auf dem Primary Domain Controller; dies ist ein entscheidender Vorteil gegenüber der dezentralen Verwaltung der Benutzer auf den einzelnen NT-Systemen einer Arbeitsgruppe. Jeder Benutzer erhielt ein eigenes Home-Directory zur Speicherung seiner Daten; die Mailbox des Benutzer wurde ebenfalls in dieser Hierarchie angelegt.

Abbildung 10 – Benutzer-Profiles

Die Verzeichnishierarchie wird über ACLs geschützt. Ferner werden die Desktop-Einstellungen (Profiles) des einzelnen Benutzers innerhalb des Home-Directories gespeichert. Diese Vorgehensweise bietet dem Benutzer eine einheitliche Sicht seiner Daten und Einstellungen von allen NT-Systemen der Domäne aus.

4.5 Datenorganisation

Als Dateisystem findet ausschließlich NTFS Verwendung. Die Verfügbarkeit der Daten kann durch die zentrale Speicherung auf dem als File-Server eingesetzten Primary Domain Controller entweder durch die in NTFS vorhandene Möglichkeit zur Konfiguration einer Software-RAID Umgebung oder durch Hardware-Optionen - RAID Controller - gesteigert werden. Neben der Reglementierung der Zugriffe auf die Benutzerdaten, lassen sich mit Hilfe der ACL-Mechanismen - Positiv- und Negativ-Listen - gezielt Zugriffe auf zentral angebotene Tools oder weitere Datenbereiche steuern. Die Sicherung des Datenbestands erfolgt zentral durch einen installierten Backup-Service. Konkret kann an dieser Stelle ADSM eingesetzt werden.

Implementierte Dateisysteme und Einsatz:

FAT16	Disketten
FAT32	nicht implementiert (NT 4.0)
NTFS	Festplatten
CDROM	CD-Laufwerke

Tabelle 2 – Dateisysteme

4.6 Zugriff auf zentrale Dienste

4.6.1 Zentrale Datensicherung

Der zentral angebotene Backup-Service ADSM kann für NT-Systeme genutzt werden. Die Installation sollte auf dem File-Server als *Service* (NT-Sprachgebrauch für Hintergrund-Prozesse) erfolgen. D.h. der NT-Rechner nimmt am zentral gesteuerten ADSM-Scheduling teil, wobei die dazu nötige Sofware-Komponente als Hintergrund-Task gestartet ist. Dieser Startvorgang kann mittels des NT-Service-Manager-GUI parametrisiert werden.

Weiterhin ist auf jeden Fall ein Satz Notfalldisketten auf einem aktuellem Stand zu halten. Diese Disketten und die CDROM-Distribution sind für das Disaster-Recovery unverzichtbar!

4.6.2 Zentrale Druckausgabe

Die NT-Betriebssysteme sind mit einer Implementierung des aus UNIX-Welt bekannten Berkeley Drucksystems ausgestattet. Diese Implementierung umfaßt sowohl die Client- als auch Server-Funktionalität. Damit kann unmittelbar auf die zentralen Druckdienste zugegriffen werden.

Zur Reduzierung des Konfigurationsaufwands können die Drucker und Treiber einmalig auf einem NT-Server, bei kleinen Arbeitsgruppen der Domain Controller, eingerichtet werden. Domänenbenutzer *ziehen* bei Bedarf mit der Maus den jeweiligen Drucker einfach auf ihren Desktop; Treiber und Einstellungen werden automatisch übernommen und aktuell gehalten. Der daraus resultierende zweifache Spoolvorgang und die damit erhöhte Netzlast sind an dieser Stelle als Preis für ein einfaches effizientes Management zu sehen.

4.6.3 PCSRV im JuNet

Ohne Installation von Zusatzkomponenten kann direkt auf den angebotenen Dateidienst (Q-Disk) zugegriffen werden, da die zentral eingesetzte Samba-Software interoperabel mit der NetBIOS-Implementierung der NT-Systeme ist.

4.6.4 X11 und NFS zur UNIX-Welt

Der X11-Zugriff und die NFS-Anbindung an beliebige UNIX-Server können für NT mit der gleichen Produktlinie durchgeführt werden, die schon für Windows 95 auf dem zentralen PCSRV angeboten wird. Im einzelnen sind an dieser Stelle zu nennen:

- PC-Xware
- Interdrive NFS Client

Andere untersuchte Produkte bieten derzeit keine weiteren Vorteile und rechtfertigten damit nicht den Umstieg auf eine andere oder zweite Produktlinie.

4.6.5 Electronic Mail

Zum Lieferumfang des Betriebsystems gehört eine Internet-Mail-Implementierung. So kann beispielsweise mit Benutzeragenten (Mail-GUIs) auf den zentral angebotenen POP-Server im ZAM zugegriffen werden. Die Installation einer eigenen POP3-Implementierung ist somit nur in begründeten Ausnahmefällen in Erwägung zu ziehen.

5 Fazit

5.1 NT-Workstation oder NT-Server

Der Betrieb von NT-Servern und NT-Workstations als Standalone-Systeme (Einbindung in Arbeitsgruppen, lokale dezentrale Benutzerverwaltung) kann im Forschungszentrum bei Bedarf in Eigenverantwortung der Organisationseinheiten ähnlich Windows 95 erfolgen. Die Verträglichkeit mit der etablierten Netzwerkstruktur und zentralen Diensten wurde ausgiebig geprüft und läßt keine prinzipiellen Probleme erwarten. Das große Angebot an Software für dieses Betriebssystem, sowohl technische als auch kommerzielle DV-Lösungen, und die zunehmende Verbreitung dieses Betriebssystems in der Industrie sprechen ebenfalls für einen Einsatz von NT.

5.2 NT-Domänen

Mit Hilfe einer vordefinierten Domänenstruktur könnte ein Angebot des ZAM an das Forschungszentrum entwickelt werden, standardisierte NT-Gruppen in den jeweiligen Instituten einzurichten (analog zu den bewährten Workstation-Gruppen) und möglichst unter Mitwirkung einer externen Firma zu betreuen. Aufgrund der Erfahrungen wird eine Struktur vorgeschlagen, die vorerst auf NT 4.0 basiert und aus unabhängigen Einzeldomänen besteht. Je nach Implementierungsstand neuer Technologien in zukünftigen NT-Versionen, insbesondere NT 5.0, können diese in einem fest definierten Zustand eingerichteten Domänen gleichartig, und damit effektiv an neue Technologien angepaßt werden. Auf die Definition von Vertrauensstellungen zwischen den Einzeldomänen soll im Hinblick auf bisherige Ankündigungen verzichtet werden. Durch fortlaufende Technologiestudien entwickelt und definiert das ZAM tragbare Lösungen für diese NT-Umgebungen.

Die Aufgaben des Primary Domain Controller in solchen Arbeitsgruppen aus 5-20 Clients wären:

- Benutzer- und Zugriffsverwaltung
- Datei-Server (Home Directories und Tools)
- Druck-Server (eigene Drucker und Weiterleitung an zentrale Druck-Server)
- Datensicherung
- Applikations-Server (beispielsweise WWW für die Organisationseinheit)

Beim weiteren Ausbau der Arbeitsgruppe sollte auf jeden Fall ein sogenannter Backup-Domain-Controller zusätzlich konfiguriert werden.

6 Ausblick

6.1 Active Directory

In NT 5.0 wird ein vollständig neu implementierter Directory Service verwendet. Der bisherige WINS steht nur aus Kompatibiltätsgründen zur Verfügung. Neben der Verwaltung von **Sicherheitsinformationen** und **Benutzeraccounts** wird die zukünftige Organisation von NT-Domänen auf Active Directory basieren. Diese neue Technologie soll die Abbildung von Unternehmensstrukturen effizienter und flexibler ermöglichen als das bisherige Domänenkonzept.

Die Verbindung zum Internet Domain Name Server, kurz DNS, wird enger. Die NT spezifischen Directory Server werden über sog. Service Resource Records im DNS und damit im Internet-Kontext bekanntgemacht. Microsoft empfiehlt den Einsatz neuer dynamischer DNS-Implementierungen nach RFC 2136. Im Forschungszentrum wird bisher eine statische DNS-Implementierung eingesetzt.

Als NT-Domänen-Namen sind gültige DNS-Namen zu verwenden.

6.2 Distributed Security Services

Flexible Möglichkeiten zur Organisation der Account-Verwaltung und die Unterstützung sicherer Internet-Kommunikation werden durch den neuen Distributed Security Service in Verbindung mit dem Active Directory Service ermöglicht. Kernkomponente ist eine Kerberos V5 Implementierung nach RFC 1510. Die bisher bekannte LAN-Manager Authentifizierung wird durch die Kerberos-Implementierung abgelöst.

6.3 Distributed File System

Das Distributed File System ist eine Server-Komponente zur Organisation von Dateisystemen in Netzwerken; dabei werden die bisher bekannten klassischen File Server Shares in einer Hierarchie-Ansicht zusammengefaßt. Diese Ansicht ist unabhängig davon, welcher File Server momentan ein bestimmtes File-Share bereitstellt.

7 Literatur

[1] Microsoft Press
Microsoft Windows NT Server Version 4 - Die technische Referenz

[2] Eric Tierling (Addison Wesley Verlag)
Networking mit Windows NT 4.0

[3] Mark Minasi (Network Press Verlag)
Windows NT Server 3.5x

[4] PC Professional Expert Edition (97-004)
Windows NT Secrets